I virus informatici

Giovanni Ziccardi

Draft v. 1.0 (2002)

1. I virus informatici: evoluzione normativa e definizioni tecniche e giuridiche.

1.1. Virus informatici ed evoluzione normativa.

La dottrina giuridica, sia in Italia sia, soprattutto, negli Stati Uniti d'America, iniziò a manifestare uno specifico interesse scientifico con riferimento al fenomeno della criminalità informatica in generale – anche se, vedremo in seguito, non ai virus informatici in particolare - già negli anni Sessanta, quando sono stati pubblicati i primi studi sui cosiddetti *computer crimes* o *computer-related crimes*.

In quegli anni, sono individuati sostanzialmente quattro comportamenti illeciti, molto generici, che si ritiene possano essere riuniti nella nozione generica di computer crimes, e che consistono:

- a) nell'attività di manipolazione di computer o di dati;
- b) nel sabotaggio di computer;
- c) nell'attività di spionaggio commessa attraverso le tecnologie informatiche;
- d) nell'utilizzo di sistemi informatici per fini contrari alla legge¹.

In queste quattro categorie elaborate dalla dottrina, non sono previste esplicitamente fattispecie criminose correlate ai virus informatici: il motivo è che in quegli anni ancora non erano stati resi noti fenomeni criminali correlati all'utilizzo di codice nocivo.

Inoltre, l'analisi della dottrina, in quegli anni, procede attraversando alcuni dubbi: in particolare, si registra una vivace discussione se questi fenomeni fossero giustificati da qualche ragione plausibile, e i primi studi empirici veri e propri sui computer crimes, compiuti con l'applicazione di metodi di ricerca scientifici criminologici e, soprattutto, analizzando anche condotte più specifiche quali quelle correlate alla diffusione dei virus informatici, non furono condotti, proprio a causa di questi dubbi, prima della metà degli anni Settanta.

Nonostante la scienza criminalistica, in questo campo, fosse solo agli inizi, questi studi portarono alla luce alcuni casi specifici di computer crimes che erano stati verificati e

¹ Per una ricostruzione storica più dettagliata dell'evoluzione, in dottrina, del concetto di computer crimes cfr., *amplius*, FONDAROLI, *La tutela penale dei beni informatici*, in «Il Diritto dell'Informazione e dell'Informatica», Milano, 1996, 291 ss., GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, PICOTTI, *Profili penali delle comunicazioni illecite via Internet*, in «Il diritto dell'Informazione e dell'Informatica», 1999, 283 ss. Id., *Fondamento e limiti della responsabilità penale dei service-providers in Internet*, in «Diritto Penale e Processo», 4/1999, 501 ss.; Id., *La responsabilità penale dei service providers in Italia*, in «Diritto Penale e Processo», 3/1999, 379 ss.; e, nella letteratura anglo-americana, BEQUAI, *Computer crime*, Lexington, 1978; FARR, *The electronic criminals*, New York, 1975; PARKER, *Crime by computer*, New York, 1976; BACKER, *Trespassers will be prosecuted: computer crime in the 1990s*, in «Computer Law Journal», 1993, vol. 12, 61 ss.; DURHAM, SKOUSEN, *The law of computer related crime in the United States*, in «American Journal of Comparative Law», 1990, vol. 38, 565.

studiati e, contestualmente, posero in evidenza un alto numero di casi non individuati o non riportati.

L'attenzione dei primi studiosi si soffermò soprattutto, su alcuni casi eclatanti di computer crimes, quali la truffa portata nei confronti dell'*American Equity Funding* e il caso tedesco *Herstatt*².

Negli anni Ottanta, invece, il panorama giuridico cambia radicalmente, soprattutto nel momento in cui gli organi di stampa provvedono a rendere pubblici casi di azioni di *hacking* e di diffusione di virus informatici e programmi *worms*³. Una novità evidente consiste nel fatto che le prime, rudimentali reti telematiche cominciano ad essere utilizzate per commettere crimini⁴. Gli anni Ottanta sono allora il periodo storico nel quale l'opinione pubblica si comincia ad avvicinare al problema dei virus informatici

Apparve inoltre chiaro che il concetto di computer crime non era più limitato all'ambito della criminalità economica, ma comprendeva attacchi contro tutti i tipi di bene giuridico come, ad esempio, la manipolazione di computer degli ospedali o la violazione informatica della *privacy*, beni giuridici la cui lesione, originariamente, era studiata in un ambito differente rispetto a quello tradizionale dei computer crimes.

La conclusione logica fu che la nozione di computer crime doveva essere la più ampia possibile, sino a comprendere, negli anni Novanta, anche i reati connessi ad Internet⁵, la distribuzione di contenuti illegali attraverso le reti telematiche e l'uso di computer e di sistemi di telecomunicazione da parte del crimine organizzato.

L'analisi degli aspetti qualitativi dei computer crimes in generale, e di quelli correlati ad Internet in particolare, ha reso pubblici i reali pericoli e le concrete minacce portate da questo tipo di criminalità⁶.

² La truffa ai danni dell'*Equity Funding* si manifestò nel corso del 1973, e riguardò la manipolazione di oltre 56.000 polizze assicurative per un valore di vendita di oltre 30 milioni di dollari. Il caso *Herstatt* riguardò transazioni speculative su valuta straniera per diversi milioni di dollari che non furono registrate nei file di *account* della banca *Herstatt*. La bancarotta della banca, nel 1974, causò una perdita ai clienti tedeschi per quasi 1 miliardo e 200 milioni di marchi.

³ In questi anni, una grande quantità di fatti criminali concernenti, ad esempio, la pirateria dei programmi per elaboratore, la manipolazione degli apparecchi distributori di denaro contante e abusi di vario genere sui sistemi di telecomunicazioni rivelarono alla comunità scientifica, e ad un vasto pubblico, la vulnerabilità della società dell'informazione e, soprattutto, l'improrogabile necessità di una nuova strategia per la sicurezza ed il controllo del crimine informatico e telematico.

⁴ Il pericolo dell'*hacking* divenne particolarmente evidente nel 1989, quando indagini dell'Autorità Giudiziaria nella Repubblica Federale di Germania identificarono alcuni *hacker* tedeschi che stavano utilizzando *network* internazionali di dati al fine di accedere a determinate informazioni all'interno di computer americani, inglesi e di altri Stati stranieri, per vendere ciò che trovavano all'interno dei sistemi informatici al KGB, il Servizio Segreto sovietico. Nello stesso periodo, il pericolo di virus e di worms divenne evidente quando l'*Internet Worm* creato da uno studente americano, Robert Morris, infettò in pochi giorni circa 6.000 computer in Internet.

⁵ Per quanto riguarda una panoramica generale, con riferimento ai crimini commessi attraverso Internet, cfr. BALLARINO, *Internet nel mondo della legge*, Padova, 1998; HANCE, *Internet e la legge*, Milano, 1997; TORRANI, PARISE, *Internet e Diritto*, Milano, 1997; TOSI (a cura di), *I problemi giuridici di Internet*, Milano, 1999, e, nella letteratura anglo-americana, BEKKERS, KOOPS, NOUWT, *Emerging electronic highways - New challenges for politics and law*, London, 1996; CAVAZOS, MORIN, *Cyberspace and law*, Cambridge, 1994; EDWARDS, WAELDE, *Regulating Cyberspace*, Oxford, 1997; KATSH, *Law in a digital world*, New York - Oxford, 1995; MACKAAY, POULIN, TRUDEL, *The Electronic superhighway - The shape of technology and law to come*, London, 1995; ROSENBERG, *Cyberlaw - The law of the Internet*, New York, 1997.

⁶ Cfr. MILITELLO, *Informatica e criminalità organizzata*, in «Rivista Trimestrale di Diritto Penale dell'Economia», 1990, p. 81 ss.

Nella comunità finanziaria ed economica, la maggior parte delle transazioni monetarie è amministrata da computer; il successo del commercio elettronico, nel prossimo futuro, dipenderà dalla sicurezza che si riuscirà ad accordare alle transazioni concluse attraverso la moneta elettronica⁷; i bilanci delle società sono redatti e gestiti con l'ausilio dei computer, e l'intera attività produttiva di molte società dipende dal corretto funzionamento del sistema di trattamento informatizzato dei dati⁸.

La maggior parte delle società memorizza i propri segreti industriali in formato elettronico, le Pubbliche Amministrazioni confidano in una tecnologia sicura che muti il volto della burocrazia all'insegna dell'efficienza, della trasparenza e del risparmio di spesa⁹, i sistemi di controllo della marina, della difesa aerea e spaziale, del campo medico dipendono oggi dal buon funzionamento della tecnologia informatica.

Le reti telematiche internazionali stanno diventando i centri nevralgici dell'economia, del settore pubblico e della società e, di conseguenza, la sicurezza delle informazioni elettroniche e la prevenzione dei *computer crimes* diventa d'importanza decisiva.

Ulrich Sieber, uno dei maggiori studiosi di queste problematiche, ha individuato nei suoi studi, nel corso di questi ultimi vent'anni, sei ondate principali di legislazioni penalistiche che oggi delimitano i sei campi principali di studio della cosiddetta *criminal information law*¹⁰ nei quali fare rientrare anche le problematiche giuridiche correlate ai virus informatici.

La prima ondata di riforma, nei sistemi giuridici occidentali, è stata registrata nel campo del diritto alla privacy ed alla sua protezione, ed ha avuto il suo culmine negli anni Settanta ed Ottanta. Questa attività legislativa è apparsa a tutti gli studiosi come un'immediata reazione alle nuove sfide portate dalla tecnologia alla privacy, grazie soprattutto alla possibilità di raccogliere, immagazzinare, trattare e trasmettere dati attraverso i nuovi strumenti informatici¹¹.

Il secondo momento di riforma legislativa ha coinvolto la repressione della criminalità economica correlata all'uso dei computer, e si è concentrato agli inizi degli anni ottanta. Questa legislazione è apparsa necessaria ai Governi di molti Paesi in quanto le previsioni criminali tradizionali tutelavano, quasi esclusivamente, oggetti fisici, tangibili e visibili.

Le nuove forme di *computer-related crimes* che iniziavano ad essere denunciate non violavano unicamente beni tradizionali (come, ad esempio, denaro depositato su conti

⁷ Cfr. FINOCCHIARO, *Il problema dei mezzi di pagamento*, in TOSI (a cura di), *I problemi giuridici di Internet*, Milano, 1999, p. 105 ss.; GAMBINO, *Gli scambi in rete*, in «Il Diritto dell'Informazione e dell'Informatica», 1997, p. 423 ss.

⁸ Cfr. fra gli altri, a questo proposito, GORE JR., *A Framework for Global Electronic Commerce*, in Internet all'indirizzo <http://www.iitf.nist.gov/elecomm/ecom.htm> (sito consultato il 15 maggio 1999); RUBERTI, *Tecnologia domani*, Roma - Bari 1985; FINKELSTEIN, *Windows on a New World. The Third Industrial Revolution*, New York, 1989.

⁹ Cfr. MINERVA, *Verso l'integrazione di sistemi informativi pubblici: la rete unitaria della Pubblica Amministrazione*, in «Il Diritto dell'Informazione e dell'Informatica», 1998, 623 ss.

¹⁰ Cfr. SIEBER, *Legal aspects of computer-related crimes in the Information Society. COMCRIME Study*, Bruxelles, 1998.

¹¹ Leggi sulla protezione dei dati personali sono state emanate, e costantemente riviste ed aggiornate, tutelando il diritto dei cittadini alla *privacy* con sanzioni amministrative, penali e civili, nel 1973 in Svezia, nel 1974 negli Stati Uniti, nel 1996 in Italia, nel 1984 nel Regno Unito, nel 1997 nella Repubblica Federale di Germania. In Australia è stato emanato il *Freedom of Information Act* del 9 marzo 1982, poi emendato dal *Privacy Act* del 1988. In Brasile, Paesi Bassi, Portogallo e Spagna la protezione della *privacy* ha portato anche ad emendamenti costituzionali. Cfr., in proposito, TAMBURRINI - FAGGIOLI, *Privacy: formulario commentato*, Milano, 1997; BUTTARELLI, *Banche dati e tutela della riservatezza - La privacy nella società dell'informazione*, Milano, 1997 e, con particolare riferimento alla *privacy* informatica, FRANCESCHELLI (a cura di), *La tutela della privacy informatica. Problemi e prospettive*, Milano, 1998.

correnti gestiti da computer) ma, anche, oggetti intangibili, quali i programmi per elaboratore, e rivelavano nuove modalità di commissione del reato (ad esempio la manipolazione di un computer, in vece del raggio di una persona, per trarre in inganno la macchina). Impossibilitati ad estendere le previsioni legislative esistenti, operazione che agirebbe in contraddizione del principio di legalità e del divieto di analogia *in malam partem*, molti Paesi hanno emanato, in questi anni, nuove leggi pensate per combattere i computer crimes correlati all'economia, con particolare riferimento agli accessi abusivi ai sistemi informatici e telematici¹².

Nel corso degli anni Ottanta, una terza serie di provvedimenti legislativi ha aumentato la protezione giuridica accordata alla proprietà intellettuale nel campo della tecnologia informatica¹³. Dopo aver escluso la protezione dei programmi per elaboratore secondo la tutela brevettuale negli anni settanta, numerose leggi di riforma hanno previsto espressamente una protezione secondo il diritto d'autore (*copyright* nei Paesi anglosassoni) per i programmi informatici (negli Stati Uniti una simile tutela è stata accordata sin dal 1980)¹⁴.

Una quarta ondata di riforme è stata operata con riferimento ai contenuti illegali e dannosi diffusi attraverso mezzi informatici, ed è iniziata timidamente nel 1980 in diversi Paesi per poi espandersi rapidamente a causa della ascesa inarrestabile di Internet che si è registrata alla metà degli anni novanta¹⁵.

Sempre a cavallo degli anni ottanta, è possibile percepire una quinta ondata di leggi nel campo della procedura penale, con nuove disposizioni che trattano problemi specifici di questo settore, quali il sequestro di apparecchiature informatiche e l'intercettazione di flussi di dati telematici.

Un'ultima azione normativa, più recente, sta attraversando il settore per far fronte alla sempre più pressante richiesta di misure di sicurezza tecniche per i dati informatici. Leggi di siffatta specie stabiliscono, ad esempio, da un lato un minimo di misure di sicurezza obbligatorie nell'interesse della tutela della privacy o dell'ordine pubblico e, dall'altro, un controllo da parte dello Stato sull'utilizzo di simili misure tecniche per un'effettiva persecuzione del crimine (come, ad esempio, la limitazione, per legge, della tecnologia crittografica).

In questa sesta ondata di leggi è possibile riscontrare un interesse del legislatore per il fenomeno dei virus e della diffusione su larga scala di programmi pensati per arrecare danni o disturbo al sistema informatico pubblico e privato ed alle reti.

Tutte queste leggi contribuiscono, analizzate in un'ottica complessiva, ad identificare ciò che il reato informatico mira a colpire, ovvero il cosiddetto bene informatico, un bene

¹² Le leggi pensate per reprimere *computer crimes* collegati all'economia furono emanate dal 1978 negli Stati Uniti e nel 1981 nel Regno Unito, e molte sono tuttora in corso di emendamento.

¹³ Cfr. VALVOLA SCELSI (a cura di), *No Copyright - Nuovi diritti nel 2000*, Milano, 1994; ALPA, *La tutela giuridica del software*, Milano, 1994; CHIMIENTI, *Lineamenti del nuovo diritto d'autore - Direttive comunitarie e normativa interna*, Milano, 1996; FRASSI, *Creazioni utili e diritto d'autore - programmi per elaboratore e raccolte di dati*, Milano, 1997; GUGLIEMMETTI, *L'invenzione di software - Brevetto e diritto d'autore*, Milano, 1997.

¹⁴ Con particolare riferimento ad Internet, cfr. BARBARISI, *La tutela della proprietà intellettuale*, in TOSI (a cura di), *I problemi giuridici di Internet*, Milano, 1999, 135 ss.

¹⁵ Emendamenti legislativi che adattano al mondo delle nuove tecnologie previsioni tradizionali sulla diffusione di pornografia, istigazione razziale e espressioni illecite e diffamazione sono stati approvati nel Regno Unito nel 1994 e in Germania nel 1997. Speciali previsioni sulla responsabilità degli *access* e *service providers* in Internet sono state emanate negli Stati Uniti nel 1996 e in Germania nel 1997.

economico che, una volta riconosciuto e protetto dalla legge, si presenta agli studiosi come un nuovo bene giuridico¹⁶.

Accanto alle protezioni di carattere puramente tecnico, che tutelano il bene informatico da aggressioni esterne, è legittimata, in molti ordinamenti, una vera e propria tutela giuridica¹⁷.

L'interesse del mondo informatico e del mondo giuridico per i *virus*, ovvero per quei programmi basati su *malicious code* – istruzioni pensate per creare effetti dannosi – è oggi di grande attualità: nel mondo delle reti, dei servizi telematici *online* 24 ore su 24, delle grandi potenze bancarie, economiche, commerciali che si sono spostate su Internet, la minaccia più grande è diventata un *software* che possa bloccare, anche solo per poche ore, l'attività di un sistema informatico.

Il termine *virus* è un termine molto generico, che non rende giustizia a software talmente diversi fra loro, sia come progettazione sia come funzionalità – tali da costruire un panorama vario, multiforme e non definibile in maniera univoca.

Chiaramente, il timore dei Legislatori e dei tecnici nei confronti dei virus è andato via via aumentando in stretta connessione con l'evoluzione della tecnologia informatica.

Le prime prese di coscienza si sono avute, infatti, quando virus o pseudo-virus hanno bloccato sistemi informatici o reti di grandi dimensioni.

Sino ad allora, anche a causa di modalità di diffusione non agevoli come quelle consentite oggi dalle reti, l'argomento virus era snobbato anche da un punto di vista legislativo.

Basti pensare che quando, negli anni Settanta, si iniziò a disegnare un quadro normativo della criminalità informatica, i virus informatici non erano ancora un problema per il legislatore.

Le varie forme di abuso degli elaboratori elettronici – nelle due specie dei *computer crimes* e dei *computer-related crimes* – sono state studiate all'interno dell'Organizzazione per lo Sviluppo e la Cooperazione Economica (Ocse) a metà degli anni Ottanta e si è iniziato ad una definizione in categorie nelle quali i virus informatici non apparivano.

Gli studi dell'Ocse sono sfociati nella Raccomandazione n. R (89) 9 del 13 settembre 1989 “sur la criminalità en relation avec l'ordinateur” da parte del Comitato dei Ministri del Consiglio d'Europa che si proponeva di dare ai Paesi Membri un quadro tipizzato e il più completo possibile di condotte che si facevano rientrare nel concetto di crimine informatico.

In particolare tale raccomandazione prevedeva due gruppi (cosiddette liste) di condotte che gli Stati erano invitati a reprimere con sanzioni penali e con interventi legislativi *ad hoc* (la cosiddetta *lista minima*) e altre condotte la cui valutazione da un punto di vista penalistico e sanzionatorio è lasciata alla discrezionalità dello Stato (la cosiddetta *lista facoltativa*).

¹⁶ Il bene informatico viene identificato, in molte leggi, come l'oggetto di un nuovo diritto di carattere reale, un bene immateriale simile alla proprietà intellettuale che viene reso oggettivo, anche in termini di puro valore economico, dal diritto stesso. Ecco allora che il bene informatico può essere oggetto di vendita o di cessione in uso, ma può anche essere oggetto di furto, di danneggiamento, di manomissione.

¹⁷ Circa la nozione di bene informatico, cfr. FONDAROLI, *La tutela penale dei «beni informatici»* in «Il Diritto dell'Informazione e dell'Informatica», Milano, 1996, 291 ss.

Sia nella lista minima (che comprendeva frode informatica, falso in documenti informatici, danneggiamento di dati o programmi, sabotaggio informatico, accesso non autorizzato a un sistema informatico o a una rete informatica in violazione delle misure di sicurezza, intercettazione non autorizzata di comunicazioni, riproduzione non autorizzata di un programma protetto o di una topografia) sia nella lista facoltativa (alterazione di dati o programmi informatici non autorizzata, spionaggio informatico, utilizzazione non autorizzata di un elaboratore o di un programma informatico protetto) non vi era alcun riferimento al fenomeno informatico, né vi erano indicate condotte che si potessero riferire precisamente ad un virus informatico.

Fino agli inizi degli anni novanta l'attenzione degli studiosi di criminalità informatica è attirata da forme quali lo spionaggio industriale, l'accesso abusivo e il sabotaggio di sistemi; il virus ancora non viene preso in considerazione come entità capace di minare la sicurezza del sistema informatico.

I virus informatici fanno il loro ingresso in dottrina con il XV Congresso dell'*Association International de Droit Pénal* (Aidp) che evidenziò la necessità di un aggiornamento delle liste previste dall'Ocse e, nella Relazione finale approvata nel settembre del 1994, amplia i tipi di abuso comprendendo anche la diffusione di programmi virus o programmi simili.

Non solo: il timore di virus diventa un timore reale, e la Relazione aggiunge la possibilità di valutazione, da parte degli Stati, se punire non solo fatti dolosi ma anche fatti colposi o che creino rischi pericolosi, mentre il Consiglio d'Europa prevedeva unicamente condotte dolose¹⁸.

Ecco allora che fra il 1990 e il 1994 il panorama cambia: non solo nelle liste dei crimini informatici appaiono anche i virus, ma la messa in circolazione di virus informatici diventa uno dei crimini tenuti in più alta considerazione in ogni sede.

Il Legislatore italiano ha avvertito l'esigenza di prevedere, nella legislazione sui computer crimes legge n. 547 del 23 dicembre 1993 (legge 547/93) una fattispecie *ad hoc* relativa ai virus, indipendente dalla fattispecie relativa al danneggiamento di dati e programmi.

Per combattere il fenomeno dei virus è stato introdotto il reato previsto dall'art. 615-*quinquies* c.p. (talaltro inserita nella sezione dedicata alla inviolabilità del domicilio), secondo il quale viene punito con la reclusione sino a due anni e con la multa sino a venti milioni chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Molto discussa, in dottrina, è la posizione di tale articolo nella sfera dei delitti contro l'inviolabilità del domicilio, ravvisando alcuni attività prodromica rispetto al reato di danneggiamento di sistemi informatici e telematici, previsto e punito dal 635-bis c.p., e quindi più idoneo ad essere inserito nei reati contro il patrimonio¹⁹. Il reato de quo si pone infatti in frequente rapporto teleologico – quale fattispecie di pura condotta rispetto ai delitti di evento di cui agli art. 635 bis o 615 ter in quanto rappresenta un antecedente tecnico e cronologico.

¹⁸ Con riferimento all'evoluzione dei tipi di reati informatici negli anni Ottanta e Novanta cfr. PECORELLA, *Il diritto penale dell'informatica*, Padova, 2000, 1-11.

¹⁹ Su questo punto molto chiara è PECORELLA, *op. cit.*, 235-237.

Autorevole dottrina ha poi operato un raffronto tra la disciplina dei virus nel nostro ordinamento e alcuni ordinamenti stranieri. Particolarmente interessante è il rapporto tra la disciplina italiana e quella prevista dal codice penale svizzero con la legge 17 giugno 1994 (disposizione che punisce non solo la diffusione e la messa in circolazione ma anche la creazione, l'importazione e il fornire indicazione sul modo di creare dei virus), dal legislatore olandese con l'art. 350 inserito con legge 23 dicembre 1992 (che prevede la punibilità delle ipotesi colpose, e dal legislatore federale statunitense con il *Computer Abuse Amendments Act* del 1994 (anch'esso prevede la punibilità di condotte colpose anche se con alcune limitazioni).²⁰

Oggi il fenomeno dei virus, con la diffusione delle reti, ha assunto una nuova importanza. La finalità di tali norme deve allora intendersi nella protezione del corretto funzionamento delle tecnologie informatiche rispetto ad una specifica fonte di rischio quale quella costituita dai virus e a prescindere dall'evento del danneggiamento, non contemplato dalla fattispecie.

Alcuni studiosi considerano i virus i più gravi tra i reati informatici, soprattutto per la loro capacità di fare danni²¹

In dottrina, la prima definizione viene attribuita a Fred Cohen, per cui il virus è un programma che infetta altri programmi modificandoli allo scopo di includere una copia di esso. Ciascun programma infettato diventa a sua volta un virus che infetta tutti gli altri programmi con i quali viene in contatto²²

1.2. Definizioni tecniche e giuridiche.

I virus sono, in linea di principio, programmi che tramite particolari istruzioni e una volta entrati in un computer sono in grado di esperire determinate azioni – dannose o meno – e di trasmettersi ad altri elaboratori.

Rientrano nelle modalità attraverso le quali si può danneggiare un sistema informatico.

a) inserimento nel sistema operativo del computer di un particolare programma, il virus

b) l'azione: può sia danneggiare sia infettare

Accanto ai virus ci sono i worm, che si riproducono incessantemente all'interno dell'elaboratore e rallentano o bloccano il sistema e le sue funzionalità.

Autorevole dottrina²³ individua tre tipi di virus:

a) i worms, caratterizzati dalla capacità di propagarsi all'interno di una rete depositando informazioni nei nodi della medesima;

b) i trojan horses, contenuti all'interno di programmi innocui e in grado di essere incoscientemente attivati dall'utente di un computer sul quale sono caricati;

²⁰ Queste interessanti analisi comparatistiche sono svolte da PECORELLA, *op. cit.*, 238-245.

²¹ Cfr. RESTA, *I computer crimes tra informatica e telematica*, Padova, 2000, 79.

²² La definizione di Cohen apparsa nel suo articolo *Computer Viruses in Computer and Security* n. 1, febbraio 1987, p. 22, è citata in Sarzana, *Informatica e diritto penale*, Milano, 1994, 93.

²³ PARODI – CALICE, *Responsabilità penali e Internet*, Milano, 55.

c) le logic bombs, programmi che contengono al proprio interno una funzione diretta a danneggiare o a impedire il funzionamento del sistema in grado di attivarsi autonomamente a distanza di tempo dal caricamento.

Il virus è costituito da un programma autonomo o da una parte di programma ordinario avente differenti finalità, ovvero ha generalmente capacità di autoriprodursi all'interno del sistema dove è stato inserito, di infettare altri programmi. Si tratta di un programma composto da una parte destinata alla riproduzione e da un'altra che deve garantire funzionalità distruttive o di disturbo.

L'azione negativa può assumere varie forme, dalla cancellazione totale dell'hard disk alla modifica di alcuni file residenti su quest'ultimo, all'alterazione dei contenuti, alla sostituzione di funzioni.

Altri autori hanno diviso i virus a seconda di altre categorie.

In particolare i virus sono programmi composti da istruzioni logiche in grado di autoreplicarsi all'interno di altri programmi residenti nella memoria di un computer progettati per svolgere azioni distruttive o disturbanti all'interno di un settore informatico e sono ascrivibili alle seguenti categorie:

- a) virus da file, che risiedono nei file eseguibili e prendono il controllo del sistema quando il file viene mandato in esecuzione
- b) virus da boot che risiedono sull'hard disk e vengono lanciati ad ogni avvio della macchina
- c) virus polimorfici che hanno la capacità di cambiare se stessi durante le infezioni
- d) virus multi partita che sono in grado di infettare sia i file eseguibili che il settore boot²⁴

Sempre secondo gli autori citati, le principali conseguenze che derivano dall'infezione di un sistema informatico possono comprendere un blocco del sistema, la perdita di produttività, la perdita di dati, la corruzione di file, malfunzionamenti, inaffidabilità di programmi, corruzione di posta elettronica²⁵.

Sono, quindi, comunemente due gli elementi caratteristici del virus informatico, ovvero la capacità di replicare se stesso con copie dotate delle medesime caratteristiche dell'originale e la capacità di attaccare altri programmi installandosi all'interno di essi²⁶

Un'altra definizione interessante²⁷ è quella tra virus distruttivi e virus disturbanti, i primi diretti a distruggere in tutto o in parte dati o programmi, ad alterare gravemente il funzionamento del sistema o addirittura a bloccarlo, i secondi a produrre interferenze non gravi ma che arrecano disturbo.

Il numero dei virus è aumentato in maniera rilevante negli ultimi anni, soprattutto per il fatto che i macro virus si prestano facilmente ad essere manipolati e a generare nuove varianti, nonché per la relativa facilità con la quale è possibile realizzarli anche da parte di scrittori non esperti. Oggi virus e relative varianti hanno superato le 20.000 unità²⁸.

²⁴ Questa suddivisione in categorie è contenuta in SERRA – STRANO, *Nuove frontiere della criminalità – la criminalità tecnologica*, Milano, 1997, 27.

²⁵ SERRA – STRANO, *op. cit.*, 27.

²⁶ Cfr. BUONOMO, *Le responsabilità penali*, in TOSI (a cura di), *I problemi giuridici di Internet*, Milano, 1999, 332.

²⁷ POMANTE, *op. cit.*, 81.

²⁸ Cfr. Virus informatici e programmi pericolosi in rete, Securitynet, Roma, 1999, 11.

Le nuove tendenze riguardano virus che colpiscono i programmi eseguibili di windows e programmi definiti backdoor o backtools che consentono l'amministrazione remota della rete e che vengono installati sul pc senza che l'operatore se ne accorga, permettono collegamenti via Tcp/IP permettendo di manipolare e controllare alcune funzioni del Pc. Quattro tendenze:

- 1) la crescente diffusione dei macro virus
- 2) la maggior diffusione dei virus tramite le reti, specialmente tramite e-mail
- 3) la propagazione degli hoax virus
- 4) i Cd Rom commerciali a larga diffusione come veicolo di grandi epidemie.

2. Il reato previsto dall'art. 615-quinquies c.p.

2.1. Il reato di pericolo ed il dolo.

I comportamenti ritenuti penalmente rilevanti dal nostro Legislatore consentono nel procurare ad altri la disponibilità di programmi virus, in quanto il conseguimento del loro possesso può preludere sia a un loro diretto inserimento nel sistema informatico sia all'ulteriore diffusione presso altre persone che potrebbero a loro volta farne uso.

Si tratta quindi di un reato di pericolo eventualmente indiretto²⁹ dal momento che dalla diffusione del virus deriva il pericolo sia di una lesione immediata del bene protetto sia di una ulteriore condotta di diffusione, consegna o comunicazione ad altri del programma che è anch'essa pericolosa in quanto potenzialmente prodromica a un utilizzo del virus per danneggiare un sistema.

La fattispecie è diretta a prevenire, prima ancora che a punire, una serie di condotte rivolte contro la funzionalità di sistemi, dati o programmi, e la rilevanza penale dei comportamenti prescinde dal verificarsi dell'evento danneggiamento.

Il legislatore non ha sanzionato la realizzazione o la semplice detenzione di programmi virus, strutturando le fattispecie illecite con una formula di ampia portata diretta a coprire tutte le possibilità di fruizione dinamica di tale tipologia.

Circa l'elemento soggettivo, si prevede un dolo generico.

Autorevole dottrina ritiene la creazione e la diffusione dei virus come attività preparatoria di ogni forma di danneggiamento via software dei sistemi informatici³⁰

2.2. L'oggetto.

Oggetto materiale delle varie condotte previste dall'articolo in questione è un programma in grado di portare danni, ovvero che abbia per scopo o per effetto quello di danneggiare un sistema informatico o telematico, dei dati o dei programmi in esso

²⁹ Cfr. PECORELLA, *op. cit.*, 236.

³⁰ Così PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 97.

contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Tale formulazione comprende sia i virus in senso stretto sia i worms sia i virus a tempo. Debbono essere idonei a danneggiare il sistema informatico nel quale vengono inseriti o i dati o i programmi utilizzati dal sistema.

Oggi i virus vengono diffusi soprattutto per posta elettronica, per cui al momento dell'apertura dell'allegato il virus parte. In questo caso si sfruttano la capacità di diffusione della posta elettronica e la involontaria attivazione da parte dell'utente con conseguente sfruttamento delle caratteristiche proprie di determinati programmi di e-mail quali Outlook di Microsoft).

Circa l'individuazione esatta della categoria di programmi, essi devono avere per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

Viene quindi equiparata a fini penali la destinazione intenzionale di un virus al danneggiamento ovvero all'alterazione del funzionamento di sistemi, dati o programmi – e quindi un comportamento caratterizzato da una specifica intenzione criminale – con la semplice possibilità che tali eventi si verifichino per effetto di un programma.

Autorevole dottrina rileva come la formulazione dell'articolo sia quantomeno inquietante non essendo in realtà così semplice ed agevole distinguere un software progettato e realizzato con l'intenzione di ledere beni giuridicamente rilevanti da un software malfunzionante ma comunque produttivo di lesioni³¹.

2.3. Codice sorgente o virus compilato

Di particolare interesse è cercare di comprendere se con riferimento alla natura del programma virus sia rilevante ai fini della norma penalistica solo un programma elaborato in un linguaggio comprensibile per l'elaboratore (compilato o eseguibile) o anche i programmi virus scritti in un linguaggio di programmazione, sorgente, che debbono essere compilati.

Secondo già citata autorevole dottrina, ammettere la rilevanza penale anche della mera diffusione di tali programmi comporterebbe un'eccessiva anticipazione della tutela penale, attraverso la repressione di una condotta troppo lontana dalla possibile lesione del bene protetto.

Inoltre il rispetto del tenore letterale del legislatore, che parla di programma informatico, non comprenderebbe le istruzioni³².

Parte della dottrina ritiene indissolubile il genus virus al concetto di programma eseguibile, atteso che solo nell'ambito di un programma di questo tipo è possibile che si installi e si riproduca un virus³³. In realtà oggi la situazione sta cambiando e non è remota la possibilità di virus allegati a immagini o file sonori, file doc o file html, applet Java o script visual basic.

³¹ POMANTE, *Internet e criminalità*, Torino, 1999, 30.

³² Cfr. PECORELLA, *op. cit.*, 248.

³³ Cfr. PARODI – CALICE, *op. cit.*, 58.

2.4. La condotta.

Circa la condotta sanzionata, si ricomprende ogni messa in circolazione di programmi infetti prevedendone sia la diffusione presso una cerchia indeterminata di persone sia la comunicazione o consegna ad una o più persone determinate.

La diffusione si ha quando il virus viene venduto, regalato o reso accessibile a tutti gli utenti di un sistema o di una rete informatica ad esempio memorizzato all'interno di un archivio elettronico dal quale sia consentito riprodurlo.

Parte della dottrina ritiene che non configuri una ipotesi di diffusione l'inserimento del programma nella memoria o nel sistema operativo di un elaboratore collegato in rete con un numero indeterminato di altri sistemi che possono essere a loro volta contagiati per via della capacità di trasmissione del codice³⁴ e si ricadrebbe nel più grave caso di danneggiamento informatico ex 635-bis.

La consegna riguarda la cessione anche fisica del supporto contenente il virus, mentre la comunicazione riguarda ad esempio l'invio via modem o via mail.

Importante è l'interpretazione della norma alla luce del principio di offensività, per cui tutte le condotte menzionate assumono rilevanza solo a condizione che siano oggettivamente idonee a creare una situazione di pericolo per i sistemi informatici altrui. Sono quindi tre le condotte differenti previste dalla normativa: diffusione, comunicazione, consegna.

Per diffusione si intende la comunicazione ad un numero potenzialmente indeterminato di soggetti (immissione in Internet, su siti) e anche immissione surrettizia del virus all'interno di un sistema con modalità tali per cui la propagazione di un medesimo possa avvenire indipendentemente e al di fuori del controllo sia del titolare del sistema sia dell'autore dell'immissione³⁵.

La comunicazione implica invece un contatto specifico tra soggetti conferenti e riceventi. Si può intendere ad esempio lo scambio telematico, via e-mail.

La consegna presuppone un contatto specifico tra soggetti, ad esempio la dazione di un supporto.

Vengono utilizzati tre termini – diffondere, comunicare, consegnare – che appaiono parzialmente in sovrapposizione fra loro al fine di abbracciare esaustivamente ogni forma di distribuzione e di circolazione dei prodotti nocivi.

L'esame della fattispecie delittuosa deve pertanto incentrarsi sull'elemento psicologico del dolo, anche se può essere difficilmente individuabile nella realtà processuale. E' infatti necessario dimostrare che l'agente era a conoscenza del potenziale lesivo del software e che aveva intenzionalmente portato a termine, con coscienza e volontà, il disegno criminoso³⁶.

3. La sicurezza

³⁴ Cfr. PECORELLA, op. cit., 250.

³⁵ PARODI – CALICE, op. cit., 87.

³⁶ POMANTE, op. cit., 31.

Il d.p.r. n. 318/99, pubblicato sulla Gazzetta Ufficiale n. 216 del 14 settembre 1999, contiene un regolamento che reca norme per la individuazione delle misure minime di sicurezza per il trattamento dei dati personali.

Sono interessanti, allora, gli adempimenti, sia giuridici sia di adeguamento dei sistemi informatici, previsti nelle righe della legge, per permettere una attività di trattamento di dati personali che sia il più possibile sicura.

Vale poi la pena di notare che il dpcm 8 febbraio 1999 ha adottato alcuni parametri ITSEC (Information Technology Security Evaluation Criteria, sistema introdotto nel 1992 dalla Commissione delle Comunità Europee) che contribuiscono a disegnare un quadro della sicurezza molto preciso. Degno di menzione, ad esempio, l'art. 41 sui requisiti di sicurezza dei sistemi operativi, dove si prescrive che il sistema operativo dei sistemi di elaborazione utilizzati nelle attività di certificazione, la generazione dei certificati e la gestione del registro dei certificati debbano essere conformi a parametri ITSEC.

Da un punto di vista più pratico, il modello di notificazione al Garante del trattamento dei dati prevede poi, in dettaglio, delle misure minime di sicurezza, operando sin dall'inizio una netta divisione a seconda che il trattamento sia eseguito con strumenti automatizzati o non automatizzati.

Nel modello, predisposto dal Garante stesso, sono previste in dettaglio le misure di sicurezza minime, suddivise fra misure organizzative, fisiche e logiche.

Le più interessanti, anche a livello aziendale, sono:

Per quanto riguarda le misure organizzative:

1. analisi dei rischi
2. prescrizione di linee guida di sicurezza
3. assegnazione di incarichi e redazione di appositi mansionari
4. formazione professionale
5. classificazione dei dati
6. registrazione delle consultazioni
7. documentazione dei controlli periodici
8. piano di disaster recovery e distruzione controllata di supporti

Circa le misure fisiche da adottare, di particolare utilità vengono indicate:

1. vigilanza della sede
2. ingresso controllato nei locali ove ha luogo il trattamento
3. sistemi di allarme e sorveglianza anti intrusione
4. registrazione ed autenticazione degli accessi
5. custodia dei supporti in contenitori sigillati
6. verifica della leggibilità dei supporti.

Infine, per quanto riguarda le misure logiche, il modello di notificazione prevede:

1. identificazione ed autenticazione dell'incaricato e dell'utente.
2. controllo degli accessi a dati e programmi
3. registrazione degli accessi

4. controlli aggiornamenti antivirus
5. sottoscrizione elettronica
6. cifratura dei dati memorizzati e trasmessi, annotazione della fonte dei dati.
7. Monitoraggio continuo e sospensione automatica delle sessioni di lavoro

Queste indicazioni possono essere un ottimo punto di partenza per verificare la situazione sicurezza all'interno dell'azienda: merita una nota il riferimento esplicito ai controlli aggiornamenti antivirus, per garantire non solo sicurezza contro accessi dall'esterno ma anche l'integrità dei dati.

La gestione della sicurezza informatica all'interno dell'azienda, come prevista dalla 675/96 e dai relativi provvedimenti di attuazione delle misure minime, prevede anche i virus e, comunque, l'adozione di idonei programmi antivirus.

Gli attacchi oggi non avvengono quasi più tramite dischetti o Cd Rom ma si propagano solitamente tramite la connessione di rete o su file condivisi.

La strategia di prevenzione richiede l'identificazione delle potenziali sorgenti di infezione e l'utilizzo di strumenti di contrasto adeguati.

I sorgenti di infezione sono supporti infetti, posta elettronica, Internet e reti.

Gli strumenti sono il software antivirus e il software per la sicurezza delle reti.

Un backup regolare dei dati dal momento che alcuni virus rendono i dischi o i file inutilizzabili.

L'aggiornamento del software in quanto ogni giorno ci sono dei virus nuovi che vengono scoperti e l'utilizzo delle reti ne favorisce la diffusione in tempi brevi.

Norme di comportamento interne e note informative affinché il personale collabori per difendersi dai virus.

Importante è anche la figura del security manager nel caso ci siano molte postazioni da controllare.

Teoricamente l'infezione da *floppy disk* infetti è la più semplice da arginare, perchè basterebbe controllare tutti i *floppy* in entrata per essere certi che il contenuto del supporto, una volta messo in circolazione in azienda, sia sicuramente privo di *virus*.

Naturalmente non è così semplice. Per i *floppy disk* può capitare che il supporto sia introdotto in azienda tramite canali diversi da quelli ufficiali, ad esempio un dipendente può portare in azienda del *software* personale che non sarà filtrato da una stazione di verifica e controllo.

È perciò consigliato proibire, anche ai sensi del D.lgs. 518/92, l'uso di programmi non distribuiti ufficialmente dall'azienda, e in ogni caso è opportuno fare controlli periodici su tutti i sistemi aziendali.

Il Cd-Rom è diventato un supporto molto diffuso, non solo per la distribuzione del *software* applicativo e di sistemi operativi ma anche per l'utilizzo di *software* multimediale, didattico, musica, giochi, ecc.

In esso purtroppo si annidano non solo *macro virus*, ma anche *virus* di Windows 9x nei programmi eseguibili.

Un Cd-Rom con un famoso 'Wargame' ha contribuito alla diffusione del W95/Marburg, in molti casi le stesse aziende distributrici provvedono ad avvisare l'utente e a fornire gli *antivirus* specifici, e non vanno sottovalutati neppure i rischi che si annidano nei Cd-Rom illegali.

Per difendersi, occorre dotare le postazioni che devono trattare dati provenienti dall'esterno del modulo antivirus per il controllo delle operazioni all'accesso e/o creare delle postazioni che eseguano la scansione di tutti i dati presenti sui *floppy disk* prima che vengano trattati all'interno dell'azienda.

Anche il Personal Computer portatile può diventare un veicolo di infezione. Proprio per la sua natura di apparecchio mobile viene utilizzato al di fuori dell'azienda in ambienti dei quali si ignora la integrità dei dati. Una volta infetto trasporta e trasmette l'infezione. Per questi motivi è necessario dotarlo della massima protezione antivirus caricando il modulo di controllo di tutte le operazioni di accesso.

L'utilizzo della posta elettronica e di Internet ha fornito ai *virus* un sistema efficace e rapido per diffondersi.

Attraverso questi sistemi i *virus* possono raggiungere direttamente qualsiasi postazione computerizzata dell'azienda, aggirando i semplici controlli statici.

Inoltre molti dei *virus* che da anni utilizzano per diffondersi i programmi eseguibili ed il *boot sector*, oggi usano anche i *file* di dati ovvero i documenti di Word ed Excel, i programmi applicativi che rappresentano i principali strumenti di lavoro negli uffici di tutto il mondo.

Di conseguenza, dopo un lungo periodo in cui la politica di difesa ed intercettazione è stata rivolta soprattutto al controllo dei programmi eseguibili (quelli con estensione .com, .exe), si è reso necessario cambiare completamente la strategia e la cultura di prevenzione.

Non dimentichiamo, inoltre, che la nascita di *virus* specifici per il sistema operativo Windows 95 e NT che infettano i file .exe rendono pericolosi anche i programmi eseguibili che possono venire scambiati tra utenti di posta elettronica.

L'uso di Internet e dei molti servizi messi a disposizione dalla cosiddetta superstrada dell'informazione si diffondono con crescente rapidità sia nelle aziende che nelle famiglie.

Programmi di utilità, giochi, musica, video e foto vengono prelevati dai siti FTP e sul *World Wide Web*, scambiati nelle aree di discussione di *Usenet*, e spesso attraverso programmi *client* come IRC che usano potenti linguaggi *script* vulnerabili agli attacchi di malintenzionati e che permettono agli utenti di ricevere in automatico del *software* da altre persone connesse allo stesso *server*.

Purtroppo un notevole numero di utilizzatori accetta trasferimenti di *file* o esegue programmi ricevuti da persone sconosciute, esponendosi così al rischio di subire l'infezione da parte di *virus* informatici, o il danno provocato da cavalli di troia e *backdoor*. Chi vuole diffondere un *virus* sa come rendere attraente il *software* e come ingannare l'utente. Per esempio, una *patch* per Internet Explorer presente su vari gruppi di discussione, spacciata come programma di aggiornamento distribuito da Microsoft, nascondeva in realtà un cavallo di troia di origine bulgara.

Di recente sono stati analizzati alcuni *macro virus* come il W97M/Groov che tra l'altro cercava di salvare la configurazione della rete interna in un file e di inviarlo al sito *Ftp* della *Frisk Software*, noto produttore di *antivirus*.

La rete ha in qualche modo stimolato e aumentato la creatività e l'attività degli scrittori di *virus*, che attraverso Internet hanno potuto diffondere vari tipi di programmi pericolosi, compresi quelli denominati 'hack tools' o *backdoor* come il 'Back Orifice' o il *NetBus*,

ovvero programmi di amministrazione remota della rete che si installano sui Personal Computer in maniera silenziosa, cioè senza fornire particolari messaggi di avvertimento agli utenti, e che una volta attivati consentono di collegarsi via TCP/IP ai computer dove siano presenti tali *backdoor*, permettendo ad eventuali intrusi di manipolare in remoto molte funzioni dei Personal Computer: prelievo e invio di *file*, esecuzione di programmi, monitoraggio di processi, appropriazione di *password* riservate.

Il tradizionale rapporto statistico EUROS - SECURITYNET sulla diffusione dei virus informatici in Italia è chiaro sul punto.

Il campione osservato nella statistica sulla diffusione dei *virus* in Italia nel 1998 è composto da oltre 1.000 utenti appartenenti ad aziende bancarie, della pubblica amministrazione, industriali e di servizi. È suddiviso e distribuito, per i vari elementi che qualificano la ricerca, in maniera omogenea, e perciò può essere considerato come sufficientemente rappresentativo del contesto nazionale.

Interessante il fatto che gli incidenti sono stati provocati da 52 diversi tipi di *virus*, ma nella pratica il 90% delle infezioni sono derivate da soltanto 15 tipi di *virus* diversi.

I 15 virus più diffusi nel nostro Paese sono noti con i seguenti nomi o sigle: Cap, Junkie, RPS2, Bye, Divina, NYB, Moloch, Peter II, Form, Laroux, Class, Parity Boot, AntiExe, Lilith, PG3.

Questi quindici *virus* insieme hanno generato l'89,97% degli incidenti segnalati. I *virus* sono stati rilevati in aziende presenti su tutto il territorio nazionale e si è registrata un'uniformità nella distribuzione regionale dei tipi di *virus* e degli incidenti.

Le principali cause della diffusione nelle aziende sono state i *floppy disk* (44% dei casi), i *networks* (51% dei casi) e i Cd-rom (5% dei casi).

Alla voce *network* vengono compresi tutti gli utilizzi della rete, tra i quali la posta elettronica interaziendale, la posta interna, la condivisione di risorse in rete, l'utilizzo di Internet.

I primi *macro virus* vennero riscontrati in Italia nel 1996 e nel 1998 hanno confermato il loro primato nella diffusione e nella causa di incidenti.

La conferma che una delle caratteristiche regnanti dei *macro virus* è quella di diffondersi rapidamente e con estrema facilità, viene anche dalla considerazione che il virus denominato Class, in pochi mesi è diventato uno fra i *virus* più comuni.

I virus di *boot* risultano ancora molto diffusi, ma vengono quasi sempre intercettati sui *floppy disk* che li ospitano e raramente esercitano i loro effetti negativi in seguito a trasferimenti sull'*hard disk*.

Lo scambio di messaggi tramite posta elettronica ha favorito anche il diffondersi degli *Hoax Virus*, ovvero di finti *virus* composti da messaggi che informano il destinatario sull'esistenza di *virus* estremamente dannosi e che si attiveranno leggendo messaggi di posta elettronica, ma che in realtà sono delle burle il cui effetto è comunque quello di bloccare l'uso del PC da parte dell'utente.

I virus più comuni sono di lunghezza variabile, fra i 1244 e 1258 *bytes*. Prima di infettare, il codice virale controlla il nome del *file* e la sua corrispondenza a qualcosa. Il *virus* solitamente risiede in memoria e infetta i *file* .com e .exe. La prima volta che un programma infettato viene eseguito, il *virus* installa se stesso in memoria e infetta vari *file*. I *files* infettati dimostrano una crescita nelle dimensioni, a volte operano danni casuali ai *files* e manipolano i *cluster* del disco fisso incrociandoli.

Altri bloccano il sistema e provocano delle ripartizioni automatiche del sistema stesso, altri riscrivono i primi settori dell'unità corrente.

Alcuni *virus* sono residenti in memoria (TSR), infettano la tavola di partizioni (*Master Boot Record*), altri mandano delle stringhe di testo ad intervalli periodici alle porte COM, altri alterano data ed ora.

Interessante come opera il *Back Orifice*. Il gruppo di hacker Cult of the Dead Cow ha rilasciato su Internet un programma chiamato 'Back Orifice' che è una *utility* per *network administrator* che permette di controllare e monitorare i computer dotati di sistema operativo Windows 95 e 98 attraverso la rete, e permette di leggere che cosa l'utente digita, cattura le immagini che sono visualizzate sul monitor, carica e scarica *files* in remoto e può indirizzare le informazioni ad un sito Internet remoto (connessione TCP/IP). Tra le funzioni più pericolose può condividere risorse, catturare le *password*, accedere al *system registry*.

Sebbene sul mercato vengano commercializzate varie applicazioni con queste caratteristiche, questo programma viene classificato come pericoloso perchè non solo può eseguire una autoinstallazione ed esecuzione invisibile permettendo così che un computer in rete con connessione TCP/IP diventi completamente controllabile e gestibile in remoto, ma anche nel caso venga installato consapevolmente da un amministratore, possiede delle funzioni che consentono di intercettare e recuperare facilmente la sessione permettendo di infiltrarsi con estrema facilità tramite Internet.

La parola '*hoaxes*' indica invece 'burle' o 'scherzi'. Gli *hoaxes* non costituiscono una minaccia concreta, ma provocano comunque una perdita di tempo e risorse. Molte organizzazioni impiegano più tempo per gestire gli *hoaxes* che per occuparsi di reali incidenti da *virus*.

Sono dei messaggi circa *virus* che in realtà sono dei falsi allarmi. A volte appaiono come allarmi lanciati da enti che si occupano della sicurezza informatica. L'obiettivo è di interrompere l'uso dei computer che ricevono il messaggio: il messaggio ipotizza, ad esempio, l'esistenza di un programma *Trojan Horse* autoeseguibile capace di distruggere l'*hard disk* e inviare copie di sé stesso a ogni indirizzo presente nella *mailbox*. In realtà leggendo il messaggio di *e-mail* non si avvia nessuna procedura e non si possono aprire *file* allegati al messaggio.

Esistono vari dettagli che permettono di identificare un *hoax*: due sono le caratteristiche che rendono credibile il messaggio e ne determinano il successo nella diffusione: l'utilizzo di un linguaggio tecnico e la credibilità della fonte di provenienza.

Se si ricevono messaggi sospetti con *file* allegati è regola di *Security* non aprire i *file* allegati (*attached*) ma di cancellarli, perchè se in allegato ci fosse un programma *Trojan Horse*, eseguirebbe funzioni che potrebbero essere distruttive.